PECB

When Recognition Matters

EXAM PREPARATION GUIDE

PECB Certified Lead Forensics Examiner

The objective of the “PECB Certified Lead Forensics Examiner” examination is to ensure that the candidate understands common commercial and open source tools that may be used during computer incident investigation and digital forensic operation, and has the knowledge and the skills to support an organization in recovering and analyzing computer forensics evidence.

The target population for this examination is:

- Computer forensic specialists
- Electronic data analyst
- Specialists in computer search and evidence recovery
- Person responsible for the application or of the enforcement of one or more laws in an organization
- Person responsible for examining media to extract and disclose data

The exam content covers the following domains:

- Domain 1: Basic Principles of Digital Evidence
- Domain 2: Fundamentals of incident response with computer forensic operations
- Domain 3: Computer Forensics Hardware Structure
- Domain 4: File Structure and Forensics Operating System
- Domain 5: Acquisition and Computer Forensics Operation
- Domain 6: Computer crime investigations and forensic examination

The content of the exam is divided as follows:

Domain 1: Basic Principles of Digital Evidence

Main objective: To ensure that the CLFE candidate can understand, interpret and illustrate the main concepts of digital evidence.

Competencies	Knowledge statements
1. Ability to understand and explain the basic components of digital evidence. 2. Ability to understand the processes of identification, collection, acquisition and preservation of digital evidence. 3. Ability to understand and provide credibility to investigation. 4. Ability to extend the analysis of digital evidence. 5. Ability to understand jurisdiction-specific requirements. 6. Ability to evaluate and classify evidence by its nature, strength and usefulness. 7. Ability to understand basic principles of digital evidence. 8. Ability to understand the key components of handling process. 9. Ability to understand the instances of handling processes. 10. Ability to understand the four requirements of digital evidence.	1. Knowledge of the purpose of digital evidence. 2. Knowledge of the activities required to maintain the integrity of digital evidence. 3. Knowledge of identification and collection process of digital evidence. 4. Knowledge of acquisition and preservation process of digital evidence. 5. Knowledge of the activities required to facilitate exchange of digital evidence between jurisdictions. 6. Knowledge of the key components of methodology applied during the digital evidence process. 7. Knowledge of methodology to manage digital evidence 8. Knowledge of investigation involving digital device and evidence. 9. Knowledge on the analysis of digital evidence. 10. Knowledge on forensic readiness. 11. Knowledge of a process creating a copy of data within a defined set. 12. Knowledge of a process of gathering the physical items that contain potential digital evidence. 13. Knowledge on information or data, stored or transmitted in binary form. 14. Knowledge on the copy of the digital evidence that has been produced to maintain reliability of the evidence by including both the digital evidence and verification means. 15. Knowledge on digital storage media, evidence preservation facility, imaging, reliability, spoilage and tampering. 16. Knowledge of auditability, repeatability, reproducibility, justifiability.

Domain 2: Fundamentals of incident response with computer forensic operations

Main objective: To ensure that the CLFE can understand computer forensics operation and determine the course of action to be followed to achieve the goal of the operation.

Competencies	Knowledge statements
1. Ability to understand computer forensic laboratory. 2. Ability to understand forensic lab preparation. 3. Ability to understand policies and procedures. 4. Ability to understand computers for forensic examination. 5. Ability to understand forensic hardware or software. 6. Ability to understand portable forensic Kit. 7. Ability to prepare and execute a computer forensics operation. 8. Ability to report verbally and by writing observations related to issues that occurred during an operation, including its computer forensics operation.	1. Knowledge of organizational goals in terms of forensic examination. 2. Knowledge of building a forensic lab based on organizational goals. 3. Knowledge of law enforcement agency and internal business requirement. 4. Knowledge of forensic that can lead to civil or criminal prosecution. 5. Knowledge of preventive maintenance to protect intellectual properties. 6. Knowledge of acquisition unit used to acquire storage image of suspect's storage media. 7. Knowledge of analysis unit used to perform analysis and search on suspect's storage image. 8. Knowledge of portable unit that can be a combination of an acquisition and or analysis unit. 9. Knowledge of procedures to apply within each step of the computer forensics operation. 10. Knowledge of documented forms, guidelines, policies and procedures about the operation of the forensic labs. 11. Knowledge of the procedures to apply when recommending corrective measures to enhance the quality of on-site procedures.

Domain 3: Forensics Computer Hardware Structure

Main objective: To ensure that the CLFE can safely handle computers, components and media containing information to be examined.

Competencies

1. Ability to identify a part of computer, understand and explain the purpose of that part and how to remove it and install it securely.
2. Ability to understand and explain the physical structure of a media and where and how the information is stored and retrieved.
3. Ability to identify most common types of media, understand and explain how to read its content and write to it.
4. Ability to understand Common Magnetic Storage of Hard Disk.
5. Ability to understand the flash memory functions.
6. Ability to understand the differences of NAD and NOR flash memory types.
7. Ability to understand Solid State Drive functions.

Knowledge statements

1. Knowledge of the characteristics of main computer parts, including shape and structure.
2. Knowledge of the main purpose of main computer parts.
3. Knowledge of the physical location where the information is stored in a media and how it is stored and retrieved.
4. Knowledge of the method used by computer forensics specialist to protect the integrity of examined data.
5. Knowledge in recovering encrypted document passwords.
6. Knowledge to bypass operating system native access control without knowing the password.
7. Knowledge of the flash memory chip that can be electronically erased and reprogrammed.
8. Knowledge of the flash memory types.
9. Knowledge on the differences between NOR and NAND flash memory types.
10. Knowledge on the wear leveling flash memory process.
11. Knowledge on the garbage collection flash memory process.
12. Knowledge on the advantages to store data on flash memory chip.
13. Knowledge on the disadvantages of Solid State Drive.
14. Knowledge on the differences between HHD and SSD storage methods.

Domain 4: File Structure and Forensics Operating System

Main objective: To ensure that the CLFE have a clear knowledge where information can be found on an electronic media or image of a media, whether it is operating system's or user information.

Competencies	Knowledge statements
1. Ability to identify different file system Forensic layers. 2. Ability to determine file system installed on the media under examination. 3. Ability to understand the anatomy of files in the context of 5 layers. 4. Ability to determine common file systems. 5. Ability to understand the common operating systems. 6. Ability to understand the differences between common operating systems. 7. Understand and explain how an operating system works. 8. Understand and explain how information is stored on a media. 9. Ability to understand the different operating systems. 10. Ability to analyze a file system and find, extract and secure information from it.	1. Knowledge of the characteristics of the different file system Forensic layers. 2. Knowledge of the function of content layer and its function. 3. Knowledge of the logical structure of various media and how and where the information is stored. 4. Knowledge of the characteristics of the most common file systems, including their name, id number, numbering with regards to operating system installed, zone and data structure. 5. Knowledge of the characteristics of the most common operating systems, including their versions, default file systems, basic tree structure and hardware requirements. 6. Knowledge of the metadata and method to extract information from it. 7. Knowledge of the function of the file name layer. 8. Knowledge of the function of the application layer. 9. Knowledge on the different common file systems. 10. Knowledge on the File Allocation Table (FAT) File System. 11. Knowledge on the differences between FAT and NTFS File System Time. 12. Knowledge on the EXT3 File System. 13. Knowledge on the Microsoft Windows. 14. Knowledge of the Linux operating systems. 15. Knowledge of the OS X operating systems developed by Apply Inc. 16. Knowledge of the Android Operating Systems. 17. Knowledge of the Apple iOS Operating System. 18. Knowledge on the three components of computer forensic operation.

Domain 5: Acquisition and Computer Forensics Operation

Main objective: To ensure that the CLFE can collect and acquire the media/device containing the evidence and use various digital forensic tools available.

Competencies	Knowledge statements
1. Understand and explain definition of collection and acquisition. 2. Ability to understand and describe the cloning process. 3. Ability to describe actions performed from a higher level of assurance of integrity. 4. Understand and describe live forensics how basically works and understand its issues. 5. Understand the conventional digital forensic approach. 6. Ability to describe the rational behind Live Forensic and to be able to justify to the authority those changes are confined within a calculated boundary. 7. Ability to understand the deciding factors based on the digital forensic case that CLFE is working on. 8. Ability to understand conventional forensic approach. 9. Ability to understand popular encoding schemes. 10. Understand Windows Digital Forensic. 11. Ability to understand investigation using Autopsy. 12. Ability to understand the Image Forensic process.	1. Basic knowledge of definitions of collection and acquisition. 2. Knowledge of basic safe techniques to acquire and preserve evidence. 3. Knowledge of the components of cloning process. 4. Knowledge of the live forensics methods and tools. 5. Knowledge on the live forensic impacts. 6. Knowledge on the conventional digital forensic approach. 7. Knowledge on the Live Forensic impacts. 8. Knowledge on performing basic memory examination. 9. Knowledge to describe practical examples on analyzing live memory. 10. Knowledge to determine what type of encodings are being used on the saved documents. 11. Knowledge on the code encoding language and standard. 12. Knowledge on the practical example on file carving. 13. Knowledge on the windows digital forensic. 14. Knowledge on the process of mounting the file. 15. Basic knowledge on recovering deleted files using autopsy. 16. Knowledge on investigation using Autopsy.

Domain 6: Computer crime investigations and forensic examination

Main objective: To ensure that the CLFE can justify the way how the evidence was acquired or left behind in an ordered, standard and forensically sound manner.

Competencies

1. Ability to understand essential digital forensic topics.
2. Ability to understand decision-making process of collection or acquisition of potential digital evidence.
3. Ability to understand additional digital forensic topics.
4. Ability to describe e-mail investigation process.
5. Ability to follow the path for web browser forensic.
6. Ability to understand the forensic emerging threats.
7. Ability to understand the Anti Computer Forensic to uncover evidence.
8. Ability to apply technologies that affect the field of Digital Forensic
9. Ability to completely and accurately report the findings including the result of the analysis of the digital evidence examination.
10. Ability to deliver complete, accurate and comprehensive documentation.
11. Ability to apply appropriate measures to assure continuity during digital forensic examinations.
12. Ability to identify and understand the presence of your audience during the presentation of digital forensic findings.
13. Ability to translate complex forensic scenarios into simple stories
14. Ability to understand the purpose of the presentation and best practices used for presenters.
15. Ability to determine what you have found in the evidence.
16. Ability to apply appropriate measures to assure continuity of possession along the path followed by the evidence.

Knowledge statements

1. Knowledge on the e-mail investigation process.
2. Knowledge on the collection of power on and off devices.
3. Knowledge on the acquisition of powered-off Digital Devices.
4. Knowledge of the path followed during the process of e-mail investigations.
5. Knowledge of the procedures including the e-mail attributes.
6. In-depth knowledge of e-mail forensic.
7. Knowledge on the web browser Forensic.
8. In-depth knowledge of all Anti forensic Techniques.
9. Knowledge of the emerging technologies that affect the field of Digital Forensic.
10. Knowledge of documentation procedures throughout the examination.
11. In-depth knowledge of the documentation procedures to CLDE professional ethics.
12. Knowledge of the audience and the ways to present to them digital forensic findings.
13. Knowledge of the complex forensic scenarios.
14. Knowledge on the translating complex forensic scenarios into simple stories.
15. Knowledge of the facts how to deliver complete, accurate and comprehensive documentation.
16. Knowledge of the best practices used in the presentation.
17. Knowledge to understand the purpose of the presentation.
18. In-depth knowledge of the measures to assure continuity during digital forensic findings.
19. Knowledge of the facts and circumstances classically taken in account to justify the examination report.
20. Knowledge to apply appropriate measures to assure the continuity of possession along the path followed by the evidence.

Based on these 6 domains and their relevance, fourteen (14) questions are included in the exam, as summarized in the following table: Insert table

			Level of Understanding (Cognitive/Taxonomy) Required					
		Points per Question	Questions that measure Comprehension, Application and Analysis	Questions that measure Synthesis and Evaluation	Number of Questions per competency domain	% of test devoted to each competency domain	Number of Points per competency domain	% of Points per competency domain
Competency/Domains	Basic Principles of Digital Evidence	5	X		2	16.67	10	13.33
		5	X					
	Fundamentals of incident response with computer forensic operations	5	X		3	25.00	20	33.33
		10	X					
		5	X					
	Computer Forensic Hardware Structure	5		X	1	8.33	5	6.67
	File Structure Forensic and Forensics Operating System	5		X	3	25.00	15	20.00
		5		X				
		5		X				
	Acquisition and Computer Forensics Operation	5	X		3	16.67	15	13.33
		5		X				
		5		X				
	Computer crime investigations and forensic examination	5	X		2	16.67	10	6.67
		5	X					
Total points		75						
Number of Questions per level of understanding			8	6				
% of Test Devoted to each level of understanding (cognitive/taxonomy)			50	50				

The passing score is established at **70%.**

After successfully passing the exam, candidates will be able to apply for the credentials of PECB Certified Lead Forensics Examiner, depending on their level of experience.

TAKE A CERTIFICATION EXAM

Candidates will be required to arrive at least thirty (30) minutes before the beginning of the certification exam. Candidates arriving late will not be given additional time to compensate for the late arrival and may be denied entry to the exam room (if they arrive more than 5 minutes after the beginning of the exam scheduled time).

All candidates will need to present a valid identity card with a picture such as a driver's license or a government ID to the invigilator.

The exam duration is three (3) hours.

The questions are essay type questions. This type of format was chosen because the intent is to determine whether an examinee can write a clear coherent answer/argument and to assess problem solving techniques. Because of this particularity, the exam is set to be "open book" and does not measure the recall of data or information. The examination evaluates, instead, comprehension, application, analysis, synthesis and evaluation, which mean that even if the answer is in the course material, candidates will have to justify and give explanations, to show they really understood the concepts. At the end of this document, you will find sample exam questions and their possible answers.

As the exams are "open book"; candidates are authorized to use the following reference materials:

- A copy of the ISO 27037:2012 standard,
- Course notes from the Participant Handout,
- Any personal notes made by the student during the course and
- A hard copy dictionary.

The use of electronic devices, such as laptops, cell phones, etc,, is not allowed.

All attempt to copy, collude or otherwise cheat during the exam will automatically lead to the exam's failure.

PECB exams are available in English. For availability of the exam in a language other than English, please contact examination@pecb.com

RECEIVE YOUR EXAM RESULTS

Results will be communicated by email in a period of 6 to 8 weeks, after taking the exam. The results will not include the exact grade of the candidate, only a mention of pass or fail.

Candidates who successfully complete the examination will be able to apply for a certified scheme.

In the case of a failure, the results will be accompanied with the list of domains in which the candidate had a low grade, to provide guidance for exams' retake preparation.

Candidates who disagree with the exam results may file a complaint. For more information, please refer to www.pecb.com

EXAM RETAKE POLICY

There is no limit on the number of times a candidate may retake an exam. However, there are some limitations in terms of allowed time-frame in between exam retakes, such as:

- If a candidate does not pass the exam on the first attempt, he/she must wait 15 days for the next attempt (1st retake). Retake fee applies.

Note: *Students, who have completed the full training but failed the written exam, are eligible to retake the exam once for free within a 12 month period from the initial date of the exam*.

- If a candidate does not pass the exam on the second attempt, he/she must wait 3 months (from the initial date of the exam) for the next attempt (2nd retake). Retake fee applies.

- If a candidate does not pass the exam on the third attempt, he/she must wait 6 months (from the initial date of the exam) for the next attempt (3rd retake). Retake fee applies.

After the fourth attempt, a waiting period of 12 months from the last session date is required, in order for candidate to sit again for the same exam. Regular fee applies.

For the candidates that fail the exam in the 2nd retake, PECB recommends to attend an official training in order to be better prepared for the exam.

To arrange exam retakes (date, time, place, costs), the candidate needs to contact the PECB partner who has initially organized the session.

CLOSING FILES

Closing a file is equivalent to rejecting a candidate's application. As a result, when candidates request that their file be reopened, PECB will no longer be bound by the conditions, standards, policies, candidate handbook or exam preparation guide that were in effect before their file was closed.

Candidates who want to request that their file be reopened must do so in writing, and pay the required fees.

EXAMINATION SECURITY

A significant component of a successful and respected professional certification credential is maintaining the security and confidentiality of the examination. PECB relies upon the ethical behaviour of certificate holders and applicants to maintain the security and confidentiality of PECB examinations. When someone who holds PECB credentials reveals information about PECB examination content, they violate the PECB Code of Ethics. PECB will take action against individuals who violate PECB Policies and the Code of Ethics. Actions taken may include permanently barring individuals from pursuing PECB credentials and revoking certifications from those who have been awarded the credential. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

SAMPLE EXAM QUESTIONS AND ANSWERS

1. After deleting a file from a FAT file system, what happen to the content of the file?

Answer

- *The content will still remain on the file system, however:*

a) *1st byte in the FAT directory entry of the file will changed to hex 0xe5*
b) *Value in the FAT indicate the clusters changed to 'unallocated'*
c) *Unless the clusters are re-used, the data residing on the blocks can be recovered*

If the deleted file was fragmented, it's possible that wrong cluster may be obtained during recovery process

2. Case Study

1. The CLFE have discovered that other than laptop and cell phones, THI also provide an additional standard USB hard drive to each of their senior employee. The standard issued USB hard drive is not encrypted and the owners are responsible to protect the issued hard drive.
THI have not done an auditing on any of the issued hard drives, nor have been keeping track of the issued hard drives on their corporate IT asset list.
Nevertheless, based on THI Information Security Policies, all senior employees are required to submit their hard drives to the IT Operation department for back up at monthly basis.

Describe what is the next course of action shall be taken by the CLFE, and why.

Answer

At this point in time, the list of evidence that need to be aquired from Mr. Jones, includes:

- *Hard disk drive from his laptop*
- *Company issued Cell Phone*

- *And the company issued USB hard disk drive.*

Notice that the IT Department is also performing backup for the management personnel, the backup date will be part of the areas of interest.

1. *Perform acquisition on all devices above.*
2. *Conduct audit to determine number of issued hard drives to Mr. Jones*
3. *Conduct audit on the back up log of Mr. Jones's company issued USB disks.*

<u>Triage</u>

CLFE shall acquire all data listed on the devices above, plus performing triage on the backup data from the IT Department. Triage process shall based on the search criterias set forth by THI management.

4. What are some of the common limitations face by the forensic examiners during keywords search? List down 5 examples:

Answer

- *Keyword search may not be useful when searching compounded files;*
- *Keyword search is based on the correct encoding, if the file is encoded in different encoding scheme, keyword search will fail. e.g. searching a 7 bit word in an 8 bit encoded file content;*
- *Keyword search may not be useful searching binary files;*
- *Keyword search is literal based. unlike regular expression, keyword search is confine to the scope of the word, e.g. if search for the word "books", we will missed out the word "book", "booking", "bookie" etc;*
- *Keyword search is useless in encrypted files.*